Co-funded by the Erasmus+ Programme of the European Union

Moduli di formazione InCyT

Sicurezza delle informazioni per i dipendenti **Unità n.: (4) Settimana 7** **Nome dell'unità (modulo): (Ingegneria sociale)**	
Attività di apprendimento	❑ **Webinar** ❑ **Esercizi** ❑ **Workshop** ❑ **Presentazione** ❑ **Altro** Webinar in streaming, testi, esercizi di autovalutazione, esercizi con risposte su forum di discussione e nell'ambito delle sessioni organizzate con il formatore/mentore, e-portfolio.
Apprendimento responsabile	• David Sommer • Ileana Amburgo
Obiettivi dell'attività di apprendimento	1. Tecniche di attacco di ingegneria sociale 2. Importanza della formazione sull'ingegneria sociale 3. Come proteggersi dagli attacchi di phishing 4. L'ingegneria sociale in una prospettiva interdisciplinare
Competenze da acquisire	• **TS3 Sicurezza della rete** • **TS4 Test di penetrazione (vulnerabilità sfruttabili)** • **SS3 Analisi cognitiva e comportamentale**
Durata dell'attività di apprendimento	2 settimane
Apprendimento requisiti	***Cosa serve?*** • Accesso a Internet • Browser Internet • MS Office365

Co-funded by the
Erasmus+ Programme
of the European Union

Informazioni sintetiche sul modulo

Descrizione
L'ingegneria sociale è una minaccia importante e molto frequente per la sicurezza delle informazioni. Questo modulo spiega brevemente il ciclo di vita dell'ingegneria sociale, come avviene un attacco e come si può prevenire. In particolare, viene descritto il phishing, uno degli attacchi di ingegneria sociale più diffusi. Molte aziende utilizzano soluzioni tecniche per prevenire gli attacchi, ma le misure tecnologiche non sono molto efficaci se il personale non viene formato in modo adeguato. Questo è uno degli obiettivi di questa unità. I discenti possono essere informati su questi aspetti leggendo il testo corrispondente, guardando i webinar in streaming e risolvendo gli esercizi al proprio ritmo. Tutti questi documenti sono presenti sulla piattaforma digitale interattiva del progetto. I discenti possono verificare le loro risposte agli esercizi di autovalutazione. Le risposte agli altri esercizi devono essere salvate sul forum di discussione corrispondente e discusse con il tutor durante l'incontro comune organizzato una volta alla settimana. Gli studenti possono lavorare in modo cooperativo con gli altri e con il tutor, in particolare durante gli incontri. Saranno aiutati a sviluppare un e-portfolio importante per la riflessione e la valutazione della formazione.

Contenuto del materiale didattico

Che cos'è l'ingegneria sociale?

L'ingegneria sociale può essere definita come la manipolazione di esseri umani, il più delle volte con l'uso di metodi psicologici, per ottenere l'accesso a dati, documenti e informazioni che l'attaccante non dovrebbe avere accesso. Diverse forme di ingegneria sociale sono state riscontrate anni fa, ma a causa dell'aumento dell'uso della tecnologia nei principali aspetti del business e della vita, le minacce sono cresciute e sono diventate un processo complesso difficile da fermare. L'ingegneria sociale è oggi una delle principali minacce alla sicurezza informatica ed è una forma efficace di crimine informatico. Le potenziali ripercussioni di un attacco sociale riuscito possono essere molto pericolose per le persone e le organizzazioni. Nel 2019, ad esempio, il phishing, una forma di crimine di ingegneria sociale, è stato responsabile di molte violazioni di dati, più di qualsiasi altro tipo di attacco.

Molti attacchi di ingegneria sociale hanno un impatto finanziario e le organizzazioni hanno perso somme considerevoli. Nel 2020, ad esempio, gli Stati Uniti hanno perso 4,2 miliardi di dollari, secondo l'FBI (Abbate, 2020).

Le aziende potrebbero subire un'interruzione dell'attività - perdita di produttività, calo del morale dei dipendenti e difficoltà di recupero per l'organizzazione. Questo processo può avere delle conseguenze: spesso viene licenziato un team di risposta agli incidenti, deve essere fornito un software di sicurezza che aiuti a prevenire attacchi futuri e i dipendenti devono essere riqualificati. Le aziende, in caso di attacco di

social engineering, potrebbero subire anche un danno di reputazione, perché i clienti non sono convinti che l'organizzazione sia in grado di proteggersi.

Importanza della formazione sull'ingegneria sociale

È difficile proteggersi dall'ingegneria sociale perché le tattiche utilizzate dagli aggressori si basano sul comportamento degli individui e se i dipendenti non hanno una formazione adeguata per riconoscere gli attacchi di ingegneria sociale, il rischio di cadere vittima è grande.

La formazione sull'ingegneria sociale può essere inclusa nei programmi di sensibilizzazione alla sicurezza e fornisce ai dipendenti le conoscenze e gli strumenti necessari per riconoscere questi tipi di attacchi e proteggere se stessi e l'organizzazione (Weßelmann, 2008).

Data l'importanza della formazione sull'ingegneria sociale per ridurre al minimo le minacce, molte organizzazioni, in particolare le PMI che dispongono di minori risorse, dovrebbero essere aiutate a prendere molto seriamente la formazione sulla consapevolezza informatica, compresa quella sull'ingegneria sociale, e offrire ai propri dipendenti la possibilità di seguirla (Mimecast Contributing Writer, 2021).

Entro il 2022, ad esempio, si prevede che il 60% delle grandi organizzazioni prenderà in considerazione la consapevolezza della sicurezza (Gartner Magic Quadrant for SAT 2019).

Ciclo di vita degli attacchi di ingegneria sociale

Spesso gli attacchi di ingegneria sociale si svolgono in più fasi. L'aggressore indaga innanzitutto sulla vittima designata per raccogliere le informazioni di base necessarie, come i punti di accesso e i protocolli di sicurezza deboli che sono necessari per l'attacco. In seguito, l'aggressore cerca di ottenere la fiducia della vittima e di stimolarla a compiere azioni che di solito non rientrano nelle pratiche di sicurezza, come ad esempio la divulgazione di informazioni sensibili o la concessione dell'accesso a risorse critiche. La Figura 1 illustra il ciclo di vita di un attacco.

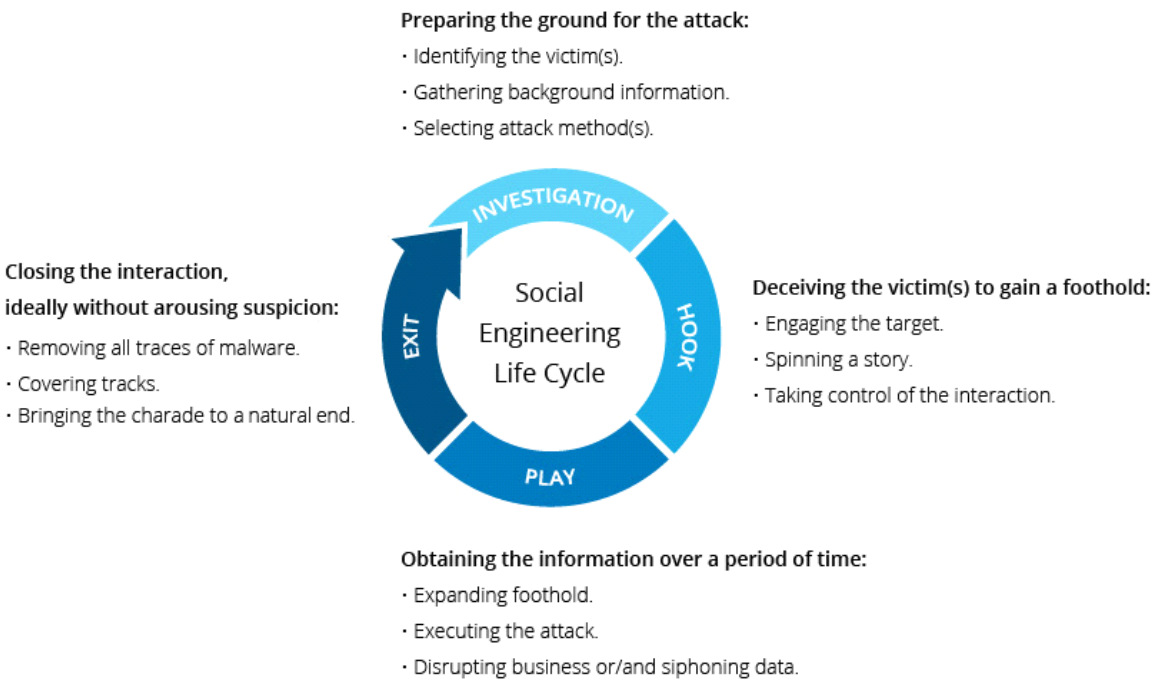

Figura 1: Ciclo di vita dell'attacco (https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/)

L'ingegneria sociale è particolarmente pericolosa perché si basa più sull'errore umano che sulle vulnerabilità del software e dei sistemi operativi. È più difficile prevedere gli errori commessi dagli utenti legittimi, identificarli e fermarli rispetto a un'intrusione basata su malware.

Tecniche di attacco di ingegneria sociale

Gli attacchi di social engineering hanno forme diverse e possono essere effettuati ovunque sia coinvolta l'interazione umana. Le forme più comuni di attacchi digitali di social engineering sono le seguenti:

Baiting attack (Attacco con esca)

Gli attacchi di adescamento cercano di attirare la curiosità della vittima. Attirano gli utenti in una trappola rubando le loro informazioni personali o infettando i loro sistemi con malware. La forma più frequente di adescamento utilizza supporti fisici per diffondere il malware. Ad esempio, chiavette infettate da malware, in aree ben visibili dove è sicuro che le potenziali vittime le vedano (ad esempio, bagni, ascensori, il parcheggio di un'azienda presa di mira). L'esca ha un aspetto autentico, come un'etichetta che la presenta come l'elenco degli stipendi dell'azienda. Le vittime raccolgono l'esca e la inseriscono nel computer di casa o di lavoro, provocando l'installazione

automatica del malware nel sistema. Gli attacchi con esca non devono necessariamente avvenire nel mondo fisico. Le forme di adescamento online consistono in annunci allettanti che conducono a siti dannosi e che incoraggiano gli utenti a scaricare un'applicazione infetta da malware.

Scareware

Le vittime diventano falsi allarmi e minacce fittizie. Gli utenti pensano che il loro sistema sia infettato da un malware e devono installare un software che ha benefici solo per l'aggressore o è esso stesso un malware. Gli scareware sono considerati come software ingannevoli, software di scansione non corretti e software fraudolenti. Un esempio comune di scareware è rappresentato dai banner popup dall'aspetto legittimo che appaiono nel proprio browser durante la navigazione in rete con un testo del tipo: "Il vostro computer potrebbe essere infettato da programmi spyware dannosi". Il testo offre l'installazione dello strumento (spesso infetto da malware) o indirizza la vittima verso un sito dannoso dove il proprio computer verrà infettato. Gli scareware vengono distribuiti anche tramite e-mail di spam che offrono agli utenti di acquistare servizi inutili/nocivi.

Pretexting (indurre a credere di essere un'altra persona)

L'aggressore ottiene informazioni attraverso una serie di bugie. La truffa (frode) è spesso avviata da un malintenzionato che ha bisogno di informazioni sensibili da una vittima per svolgere un compito critico. L'aggressore di solito inizia a stabilire un rapporto di fiducia con la vittima spacciandosi per collega, poliziotto, funzionario di banca o fiscale o altre persone che hanno il diritto di sapere. L'aggressore pone le domande necessarie per confermare l'identità della vittima, attraverso le quali raccoglie importanti dati personali. Con questa frode si possono raccogliere molte informazioni e registrazioni importanti, ad esempio numeri di previdenza sociale, indirizzi personali e numeri di telefono, registrazioni telefoniche, date di ferie del personale, registrazioni bancarie e persino informazioni di sicurezza relative a un impianto fisico.

Phishing

È uno dei tipi di attacco di ingegneria sociale più diffusi; le truffe (frodi) di phishing sono e-mail e campagne di messaggi di testo che mirano a incuriosire o spaventare le vittime e a incoraggiarle a fornire informazioni sensibili, a cliccare su link a siti web dannosi o ad aprire allegati che contengono malware. Un esempio è un'e-mail inviata agli utenti di un servizio online che li avvisa di una violazione delle policy che richiede un'azione immediata, come ad esempio la modifica della password. Include un link a un sito web non legittimo - quasi identico nell'aspetto alla sua versione legittima - e l'utente inserisce le proprie credenziali attuali e la nuova password. Le informazioni vengono inviate all'aggressore. Poiché i messaggi identici, o quasi, vengono inviati a molti utenti nelle campagne di phishing, il loro rilevamento e blocco è più facile per i server di posta che hanno accesso alle piattaforme di condivisione delle minacce.

Spear phishing

Si tratta di una forma particolare di attacco di phishing, in quanto l'aggressore sceglie persone o imprese specifiche. Gli aggressori adattano i loro messaggi alle caratteristiche, alle posizioni lavorative e ai contatti delle vittime per rendere l'attacco meno evidente. Lo spear phishing richiede uno sforzo maggiore da parte dell'autore dell'attacco (la persona che commette l'atto illegale) e può richiedere settimane e mesi di preparazione. È molto difficile rilevare questi attacchi e le loro percentuali di successo sono migliori. A titolo di esempio, uno scenario di spear phishing prevede un aggressore che, come consulente informatico di un'organizzazione (esistente), invia un'e-mail a uno o più dipendenti. Il messaggio è firmato esattamente come fa normalmente il consulente e i destinatari pensano che si tratti di un messaggio autentico. Il messaggio richiede alle vittime di cambiare la password e fornisce loro un link che le reindirizza a una pagina dannosa dove l'aggressore ruba le loro credenziali.

Rilevare il phishing

I truffatori (persone che fanno affari fraudolenti) utilizzano e-mail o messaggi di testo per ingannare le persone a comunicare le loro informazioni personali. Cercano di rubare password, numeri di conto o numeri di previdenza sociale. Se riescono a ottenere queste informazioni, possono ottenere l'accesso alla posta elettronica, alla banca o ad altri account. I truffatori lanciano migliaia di attacchi di phishing ogni giorno e spesso hanno successo. I truffatori aggiornano spesso le loro tattiche, ma ci sono alcuni segnali che aiutano le vittime a riconoscere un'e-mail o un messaggio di testo di phishing, come i seguenti:

- Le e-mail e i messaggi di testo di phishing possono sembrare provenienti da un'azienda che conoscete o di cui vi fidate. Sembrano provenire da una banca, da una società di carte di credito, da un sito di social network, da un sito o da un'applicazione di pagamento online o da un negozio online.

- Le e-mail e i messaggi di testo di phishing spesso raccontano una storia per indurre le vittime a cliccare su un link o ad aprire un allegato. Possono dire di aver notato alcune attività sospette o tentativi di accesso, affermare che c'è un problema con l'account o con le informazioni di pagamento, dire che la persona deve confermare alcune informazioni personali, includere una fattura falsa, volere che la persona faccia clic su un link per effettuare un pagamento, dire che la persona ha diritto a registrarsi per un rimborso governativo, ecc.

La Figura 2 mostra un esempio reale di phishing.

L'e-mail sembra provenire da un'azienda che la persona conosce e di cui si fida: Netflix. Utilizza persino il logo e l'intestazione di Netflix.

L'e-mail dice che il proprio account è in attesa a causa di un problema di fatturazione.

L'e-mail ha un saluto generico, "Ciao caro". Se la persona ha un account presso l'azienda, probabilmente non userebbe un saluto così generico.

L'e-mail invita la persona a cliccare su un link per aggiornare i dati di pagamento.

Questa e-mail potrebbe sembrare vera, ma non lo è. I truffatori che inviano e-mail come questa non hanno nulla a che fare con le aziende che fingono di essere. Le e-mail di phishing possono avere conseguenze reali per le persone che forniscono ai truffatori le loro informazioni. E possono danneggiare la reputazione delle aziende che simulano.

Proteggersi dal phishing

I filtri antispam delle e-mail sono in grado di tenere molte e-mail di phishing fuori dalla propria casella di posta. Ma i truffatori cercano sempre di superare in astuzia i filtri antispam, quindi è utile aggiungere ulteriori livelli di protezione.

Metodi di protezione:

- Per proteggere il proprio computer utilizzando un software di sicurezza, il software deve essere aggiornato automaticamente per far fronte alle minacce alla sicurezza.

- Per proteggere il proprio telefono cellulare, il software deve essere aggiornato automaticamente.
- Per proteggere i propri account, è necessario utilizzare l'autenticazione a più fattori.

Le credenziali aggiuntive per accedere al proprio account possono essere raggruppate in:

- Il codice di accesso si ottiene tramite un'app di autenticazione o una chiave di sicurezza.
- Una scansione della propria impronta digitale, della retina o del volto.

L'autenticazione a più fattori rende più difficile per i truffatori accedere ad altri account se ottengono il nome utente e la password corrispondenti. È importante proteggere i propri dati con backup non collegati alla rete domestica. I file del proprio computer dovrebbero essere copiati su un disco rigido esterno o su un cloud storage. Anche i dati del proprio telefono dovrebbero essere copiati.

Comportamento in caso di sospetto di attacco di phishing

- Se arriva un'e-mail o un SMS che chiede di cliccare su un link o di aprire un allegato, chiedete: Ho un account con l'azienda o conosco la persona che mi ha contattato?
- Se la risposta è "No", potrebbe trattarsi di una truffa di phishing. Dovete rivedere i suggerimenti in Come riconoscere il phishing, cercare i segni di una truffa di phishing, segnalare il messaggio e poi cancellarlo.
- Se la risposta è "sì", contattate l'azienda utilizzando un numero di telefono o un sito web reale senza inserire le informazioni nell'e-mail, perché gli allegati e i link possono installare malware dannosi.

Rispondere a un'e-mail di phishing

Ci sono dei passi specifici da fare in base alle informazioni perse

- Eseguire una scansione.
- Se si riceve un'e-mail o un messaggio di testo di phishing, segnalarlo.

L'ingegneria sociale in una prospettiva interdisciplinare

Il mondo di oggi, caratterizzato dalla rete e dall'uso intensivo di Internet e della tecnologia, è un catalizzatore di attacchi di social engineering. Le protezioni di sistema sono utili per mitigare alcuni attacchi di social engineering, ma non sono sufficienti. Il Federal Bureau of Investigation's Internet Crime ha sottolineato l'aumento dell'uso di schemi di social engineering e di frode via e-mail per le aziende, che hanno causato perdite per miliardi di dollari negli ultimi anni (Abbate, 2020). Anche in

questo caso, per quanto riguarda i metodi degli hacker, è necessario utilizzare un approccio interdisciplinare per comprendere questo fenomeno e tutte le sue complessità, soprattutto nel contesto di come influisce sulle imprese. Le rassegne della letteratura evidenziano le prospettive di diverse discipline: informatica, psicologia, economia ed etica. La Figura 3 illustra questa visione (Washo, 2021).

Disciplina informatica

L'ingegneria sociale non può essere discussa se non nel contesto degli effettivi sistemi informativi e del loro utilizzo in azienda. Le difese tecniche possono essere utilizzate come forma di mitigazione del rischio e si raccomanda l'uso di strategie di controllo. L'autenticazione a più fattori è un modo comune e spesso efficace per le organizzazioni di confermare che la persona che accede ai sistemi abbia effettivamente tale accesso. Ad esempio, un processo di login con nome utente e password è un modo per autenticare l'utente. Un ulteriore fattore potrebbe essere l'uso di una rete privata virtuale (VPN) per convalidare ulteriormente l'utente.

Disciplina psicologica

L'ingegneria sociale è legata all'inganno, quindi un approccio psicologico alla comprensione del concetto è importante per capire i pensieri e i comportamenti dell'attaccante e della vittima. L'uso di metodi psicologici è importante per l'ingegneria sociale perché vengono utilizzati per supportare le protezioni come i firewall e i sistemi utilizzati per identificare gli intrusi (Bullee, Montoya, Pieters, Junger, & Hartel, 2018). L'intera rete informatica di una determinata azienda è forte quanto il singolo utente di un determinato sistema. Infatti, il comportamento e le azioni dei dipendenti sono una delle principali cause di violazione dei dati.

Prospettiva aziendale

L'ingegneria sociale ha un impatto su molti tipi di aziende e ha implicazioni sul modo in cui le organizzazioni sono strutturate e gestite. L'argomento può essere considerato dal punto di vista aziendale per determinare i fattori che influiscono sugli attacchi di social engineering. Questo punto di vista è vantaggioso se si riferisce alle seguenti aree aziendali: formazione e sviluppo, politiche documentate, procedure di revisione interna, budget e cultura organizzativa. Una carenza in una di queste aree può contribuire agli attacchi.

Prospettiva etica

L'etica è importante nel contesto dell'ingegneria sociale e della relativa ricerca sull'argomento. L'idea di manipolare un altro essere umano viola molti principi etici. Nel caso di un evento di ingegneria sociale, il trattamento delle vittime può variare, ma spesso non sono trattate in modo sufficiente per consentire l'attacco. Purtroppo, le qualità che di solito si trovano nei dipendenti ideali, come la fiducia, la disponibilità a compiacere gli altri, come i manager, i clienti, i colleghi e i

visitatori, e la disponibilità a obbedire all'autorità, sono di solito le stesse caratteristiche che rendono un individuo suscettibile all'ingegneria sociale (Mouton, Malan, Kimppa, & Venter, 2015).

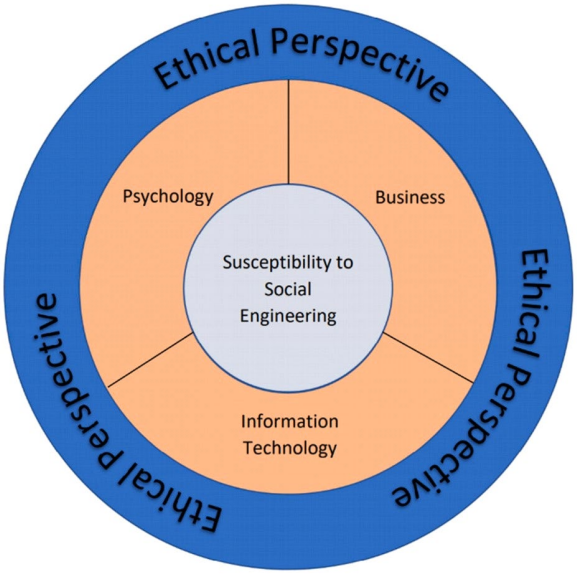

Figura 3: Ingegneria sociale da una prospettiva interdisciplinare (Washo, 2021)

La rassegna della letteratura di diverse discipline spiega la necessità di un approccio integrato per studiare il complesso argomento dell'ingegneria sociale. Ogni disciplina fornisce informazioni su come comprendere e interpretare l'argomento, proteggersi da vari tipi di attacchi e comprendere l'impatto dell'ingegneria sociale dal punto di vista umano e organizzativo. Tuttavia, l'interpretazione di ciascuna disciplina è utile solo se vista nel contesto delle altre discipline.

Domande:

Domande Forum di discussione a cui rispondere con una breve spiegazione.

1. Come riconoscere il Phishing: le e-mail e i messaggi di testo di phishing spesso raccontano una storia per indurre le vittime a cliccare su un link o ad aprire un allegato.
2. Come proteggersi dagli attacchi di phishing
3. Indicate alcune discipline collegate all'ingegneria sociale e spiegate brevemente queste connessioni.

Allegati:

1. Presentazione
2. Filmati

Riferimenti:

Abbate, P., (2020). Rapporto sulla criminalità in Internet 2020
URL: (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. *Journal of investigative psychology and offender profiling*, *15*(1), 20-45. URL: https://onlinelibrary.wiley.com/doi/10.1002/jip.1482

Lee, T. (2020). Assumere gli insegnanti giusti per una migliore consapevolezza della sicurezza. URL: https://www.gartner.com/smarterwithgartner/hire-the-right-teachers-for-better-security-awareness

Mimecast contributing writer (2021). Formazione sulla consapevolezza dell'ingegneria sociale per i dipendenti. URL: https://www.mimecast.com/blog/what-is-social-engineering/

Mouton, F., Malan, M., Kimppa, K. e Venter, H. (2015). Necessità dell'etica nella ricerca sull'ingegneria sociale. Computers & Security, 55, 114-127. https://doi.org/10.1016/j. HYPERLINK "https://doi.org/10.1016/j.cose.2015.09.001"cose.2015.09.001

Washo, A. (2021). Una visione interdisciplinare dell'ingegneria sociale: Una chiamata all'azione per la ricerca. URL:
https://www.researchgate.net/publication/353448049_An_interdisciplinary_view_of_social_engineering_A_call_to_action_for_research

Weßelmann, B. (2008). Maßnahmen gegen Social Engineering: La formazione deve essere finalizzata alla sensibilizzazione. In: Datenschutz und Datensicherheit. DuD. 601-604.